After the Medicare breach, we should be cautious about moving our health records online

July 7 2017, by Robert Merkel

How did a journalist manage to buy their own Medicare details on the dark web? Credit: AAP Image/Dave Hunt

The Australian government is digitising the country's health system, but a serious Medicare security breach suggests we may not be ready.

The Australian Federal Police are investigating after the Guardian discovered that the Medicare card details of Australians were available

for purchase on the "dark web".

The dark web – a collection of websites that are only accessible through anonymising systems such as Tor – allows vendors to remain largely hidden from law enforcement. There is a long-standing trade in illicit goods and services, including hacked personal data, on eBay-like dark web marketplaces.

As journalist Paul Farrell pointed out, criminal groups can use Medicare numbers to create fake Medicare cards with the details of real people. In combination with other personal information, these cards or simply the Medicare numbers themselves, could be used to commit a wide variety of fraud.

The Medicare system has security issues, but the number of fallible people and systems who will have access to our medical records in the future is also concerning.

Security weaknesses

It is not yet clear how the Medicare details were obtained. In a press conference on Tuesday, Minister for Human Services Alan Tudge said he had been advised "that there has not been a cyber security breach of our systems as such, but rather it is more likely to have been a traditional criminal activity".

He would not explain what "traditional criminal activity" might include, but emphasised that the Medicare details available were insufficient to gain access to personal health records.

In my view, the Department of Human Services's (DHS) Health Professional Online Services (HPOS), which provides health professionals with access to Medicare details, has weaknesses in its

security.

HPOS is an online system for healthcare and disability service providers, such as medical practices, to interact with the department, including by electronically submitting Medicare claims. It can also be used to find a patient's Medicare card number based on their name and date of birth.

Any staff member at a healthcare provider with a HPOS login as well as somebody's name and date of birth can look up the Medicare number of anyone in Australia. This matches the details requested from Farrell by the dark web vendor.

> I purchased my own Medicare card details from the Darkweb auctioneer for just $20USD. The vendor even uses a fake Aus gov logo pic.twitter.com/k5Ghk05QKK
>
> — Paul Farrell (@FarrellPF) July 3, 2017

Importantly, the mechanism for protecting HPOS from unauthorised logins does not follow modern security practices. Logins to HPOS are managed through another online system called Provider Digital Access (PRODA). This was recently rolled out as an alternative to Human Services Public Key Infrastructure certificates (PKI) that also give access to online services.

PRODA uses "two-factor authentication" to, in theory, ensure that simply stealing a username and password is insufficient to gain illicit access.

Many people are now familiar with two-factor authentication codes sent via SMS when using online banking, or authentication apps on smartphones that generate a secret code used to log in. PRODA offers both options. However, it also supports sending the code via email.

Even SMS-based two-factor authentication has security problems sufficient for the US National Institute of Standards and Technology to no longer recommend it for new systems. However, it is much better than email-based two-factor authentication. Sending a "secret token" via email is almost completely useless as a security measure.

Any compromise of a computer used for HPOS access, which gives a criminal access to the PRODA username and password, would likely give access to the email account to which the PRODA authentication codes are sent. Subsequent accesses to HPOS by the criminal would merely require them to use the stolen username and password, and to monitor the compromised email account.

In response to a request for comment, a DHS spokesperson said HPOS was designed "with security at the forefront".

"Health providers must undergo a stringent registration process to gain access to HPOS," she said in an email. "Access is granted to individuals (not to whole medical practices) when they have proven their credentials.

"The department treats the security of personal data extremely seriously and conducts thorough investigations into any claims of misuse."

Medicare numbers and mission creep

The technical flaws in HPOS and PRODA can probably be fixed over time. However, this may not be sufficient to protect Medicare numbers.

At its foundation, HPOS gives thousands of potentially corruptible and fallible humans, at locations across the country with variably-maintained IT systems, access to Medicare numbers.

Even if the department's systems can be secured, Medicare numbers are

also stored on the practice management systems of those thousands of providers.

As such, keeping them completely secure from criminals with the scent of Bitcoins in their nostrils is likely an exercise in futility.

Rather than insisting on perfect security for an insecure number, it may be more fruitful to limit the harm from its misuse. Medicare cards, for instance, can be used as part of a 100-point ID check. Perhaps it's time to consider whether this kind of extended use is appropriate.

My Health Record: a security challenge

Over the next few years, the scope of medical information held by the federal government will expand greatly.

My Health Record is a program for a centralised, electronic medical record. While it is currently an opt-in system for most Australians, in 2018 it will switch to an "opt-out" model.

Medical professionals can access patient details from My Health Record without patient authorisation in an emergency, and the system faces many of the same personnel and organisational risks as HPOS.

The sheer number of people and systems with access makes it almost impossible to keep this much more sensitive data wholly secure, regardless of the detailed technical protective measures taken.

The Medicare data breach, as serious as it is, is also an advance warning of the much greater risks we are about to run.

For what it's worth, I opted out of My Health Record for my daughter after her birth, and will do the same for myself when it's rolled out

nationally.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: After the Medicare breach, we should be cautious about moving our health records online (2017, July 7) retrieved 5 July 2024 from https://medicalxpress.com/news/2017-07-medicare-breach-cautious-health-recordsonline.html